Check for updates

Original Research Article

BIG DATA & SOCIETY

Big Data & Society
July–December 2017: 1–14
© The Author(s) 2017
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/2053951717742419
journals.sagepub.com/home/bds
SAGE

The place of conditionality and individual responsibility in a "data-driven economy"

Pascal D König

Abstract

Advances in information and communication technologies enable more decentralized and individualized mechanisms for coordination and for managing societal complexity. This has important consequences for the role of conditionality and the idea of individual responsibility in two seemingly unrelated policy areas. First, the changing information infrastructure enables an extension of conditionality in the area of welfare through greater activation, enhanced self-management, and a personalization of risks. Second, conditionality and personal responsibility also form an important ideational template and a legitimatory basis for facilitating value creation that is based on data as a raw material. This argument is illustrated looking at the trajectories of the digital strategies in the United Kingdom and Germany. In both cases, data protection is depicted as a question of individual responsibility and tied to certain forms of individual conduct.

Keywords

Digital economy, information and communication technologies, conditionality, individual responsibility, data protection, value creation

Introduction

The politics of welfare state reform is seemingly unrelated to governments shaping the conditions of data-based value creation. However, the former has a particular relevance as a template for the latter due to how conditionality, i.e. making the entitlement to protections and benefits conditional on certain kinds of behavior, and the ideal of personal responsibility have been applied in the welfare state. The principle of conditionality has taken a prominent place in welfare reforms of various industrialized countries; governments in Sweden, the Netherlands, Germany, and the United Kingdom, among others, have extended conditionality since the 1980s through tying benefits to individuals showing a certain work-related conduct (Bonoli and Natali, 2012; Hemerijck, 2013). These policies have been accompanied—in rhetoric as much as design—by a strong emphasis on individual responsibility.

More recently, government's possibilities for establishing conditionality are taken to a new level. With advances in digital technologies particularly since the 1990s, governments have seen important changes in the resources and tools at their disposal, especially in terms of nodality or information (Hood and Margetts, 2007). As information and communication technologies (ICTs) lead to a far-reaching transformation in societies' information infrastructure, more decentralized and individualized mechanisms for coordination can be used to manage societal complexity (Cukier and Mayer-Schoenberger, 2013; Helbing, 2015), with important consequences for the role of conditionality and the idea of individual responsibility. As will be argued below, individual responsibility and conditionality link the areas of welfare and of data protection in two ways against the backdrop of the changed information infrastructure: On the one hand, this

Goethe-University Frankfurt, Germany

Corresponding author:
Pascal D König, Department of Political Science, Goethe-University Frankfurt, Theodor-W.-Adorno-Platz 6, Frankfurt am Main D-60629, Germany.
Email: p.koenig@soz.uni-frankfurt.de

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (http://www.creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

infrastructure support the extension of conditionality in the area of welfare in various ways. On the other hand, responsibility and conditionality are also strengthened with regard to individuals' management of their data exposure. Specifically, as governments are compelled to support data-centered economic value creation—or simply a "Data Economy" (European Commission, 2017)—as an important factor of economic growth and international competitiveness (Colecchia et al., 2014; European Commission, 2017), they are inclined to create a suitable environment for this kind of activity (Srnicek, 2017; Zysman and Breznitz, 2012). Doing so, however, involves not only to commodify personal data as a raw material. It may also have commodifying effects on individuals as carriers of that data, subject them to heightened power asymmetries, and expose them to inconveniences and risks due to widespread practices of data collection and processing. In short, the growth of a data economy comes into conflict with socially accepted ideas of personal autonomy.

In order to deal with and overcome such legitimatory pressures, governments are likely to resort to already existing and familiar legitimizing ideas (Abdelal et al., 2010; Blyth, 2003; Hall, 1993). The politics of the welfare state provides such a template in the form of conditionality and its emphasis on individual responsibility (see, e.g., Halvorsen, 1998). The normative ideal of self-reliance and personal responsibility has underpinned changes in the welfare state toward less state intervention and an extension of the scope of market forces. In a similar vein, this ideal can be invoked with regard to data collection and processing in order to free up data flows: specifically, through shifting responsibility to the individual while sticking to a legitimizing idea of autonomy. As policy actors push the boundaries for value creation based on data collection and processing, we can thus expect to increasingly see justifications that explicitly draw on individual responsibility and that resemble those used in a rhetoric for defending welfare cuts. How individual responsibility is invoked as a legitimizing ideal for lowering restrictions with regard to data collection and processing is illustrated looking at the United Kingdom and Germany. They are chosen as two countries that recently updated their digital strategies and that have so far shown different approaches to data-driven business and privacy. Altogether, the paper thus makes two contributions to the literature: First, it connects two different strands of research and policy areas, namely welfare state research and a still very heterogeneous literature concerned with issues of privacy, data collection, processing, and protection. Second, it shows which role conditionality and individual responsibility play in an emerging data economy.

The following section will first deal with conditionality and individual responsibility in welfare state politics and with the way in which conditionality is extended in that area based on a changed information infrastructure. Section "Conditionality in data collection and processing" deals with the place of agency and individual autonomy in the political economy of data collection and processing. The final section gives a summary and a brief outlook.

Conditionality and individual responsibility in the welfare state

Conditionality in old and new politics of the welfare state

The principle of conditionality plays a pivotal role in the area of the welfare state. Conditionality implies that citizens have to show a certain conduct in order to obtain support through protections and benefits. It thus provides an answer to the question how economic resources and benefits should be allocated in a society based on specific criteria of deservingness. These standards of deservingness are heavily informed by the prevalent ideal of personal autonomy and self-reliance, which in Western industrialized societies has a predominantly economic connotation (Halvorsen, 1998). According to that ideal, those who are not or do not aim to be self-reliant but are dependent upon others count as less deserving of assistance. Conditionality in this view amounts to tying the provision of welfare benefits to one's participation in the economy—citizens are expected to take responsibility and engage in certain activities deemed relevant for entry into the labor market if they do not want to see their social rights curtailed.

This association between conditionality and the idea of individual responsibility is important because it means that the existence and extension of conditionality can be justified through invoking a normative ideal of autonomy. A historical expression of this legitimatory role of personal responsibility can be seen in the Elizabethan Poor Laws, which established a distinction between the deserving and undeserving poor. Generosity to the deserving poor was justified by the fact that they were willing to work but incapable of doing so (e.g., the handicapped). Stressing the ability to work in this fashion, however, went hand in hand with depicting those who were poor but capable of working as undeserving—the thought being: as they are basically able to provide for themselves their conditions are to be seen as the result of a lack of individual responsibility and thus a case of moral deficiency (Soss et al., 2011: 85–86). Denying a certain group among the poor benefits could thus be justified based on a normative standard.

Conditionality understood as a policy tool thus serves a twofold role. On the one hand, it models

relations between citizens and the state after a contract, according to which citizens have specific rights and responsibilities. In doing so, it appeals to the ideal of self-reliant individuals and aims to exact behavioral change in a direction that is deemed desirable. On the other hand, it also has a legitimizing function as it shifts responsibility to the individual and allows for scaling back the role of state. An extensive literature on welfare state reforms has shown that the ideas of deservingness and individual responsibility have been used in order to legitimize cutbacks and a weakening of protections in the welfare state (Cox, 2001; Kurzer, 2013; Schram and Soss, 2001; Wiggan, 2012). These kinds of justifications could be observed in countries, such as the United Kingdom, the USA, Sweden, Denmark, the Netherlands, and Germany. In all these cases, governments depicted certain recipients of welfare benefits as dependent and undeserving to justify cuts in the welfare system. Most notably governments in the United Kingdom and the United States emphasized welfare dependency as an undesirable personal characteristic. With their policies and rhetoric, they evoked the suspicion that recipients were undeserving and that the existing welfare system undermined self-reliance. At the same time, these efforts of legitimizing welfare state reform present dependency and participation in the workforce as a matter of merely individual choice and effort. The individualistic nature of the idea of a contract after which conditionality is modeled deemphasizes the role of structural conditions that may hamper individual's attempts to realize the ideal of agency as self-reliance.

Summing up, policy actors can legitimize a stronger conditionality and cuts in the welfare state as it is tied to the normative ideal of autonomy as self-reliance and to the aim of helping individuals to become productive members of society. This justification is clearly not new and has a long tradition in welfare state politics.However, the changing information infrastructure in industrialized countries makes possible new manifestations of conditionality in the area of welfare. In addition, as will be argued below, it forms an occasion for extending the principle of conditionality—serving as a suitable template—to processes of data collection and processing.

A new information infrastructure and conditionality in welfare

Ultimately, the possibility of introducing conditionality in welfare constitutes an information problem since making the provision of benefits conditional on certain criteria and assessing whether someone counts as deserving require information about individual behavior. In this sense, welfare state policies are related to developments in the information infrastructure on a fundamental level (see also Braman, 2006: 32–45), and the changes in the information infrastructure mentioned at the outset are highly relevant for welfare state policies. Specifically, the heavily increased capacities for monitoring and coordinating individual behavior amount to a significant change in the possibilities for establishing conditionality and putting greater weight on personal responsibility in managing welfare risks. These possibilities are rooted in the combination of the internet, mobile computing, and advances in sensor technology that have massively boosted the capacities for generating, distributing, storing, and processing digital information (Hilbert and Lopez, 2011; Kitchin, 2014). The information infrastructure that is created through these capacities marks a change in kind and not just in degree in two regards. First, the immediacy, responsiveness, and copresence of many entities made possible by ICTs allow for a dynamic and decentralized forms of coordination on an unprecedented scale (Bennett and Segerberg, 2012; Svensson, 2011). A multitude of individuals can coordinate their actions toward a given goal almost in real time. Second, the potential to collect immense amounts of very fine-grained data about individual behaviors and dispositions cheaply and unobtrusively has grown dramatically. The result is a growing datafication of social reality (Baruh and Popescu, 2017: 581; Chandler, 2015: 836) in the sense of detailed machine-readable representations of that reality becoming possible. In a number of areas, such as traffic or energy use, the capacity to register the minutiae of individual behavior and social processes and gain data of much higher granualarity eliminates the necessity to rely on aggregate information. These massive amounts of fine-grained data enable a monitoring of all kinds of activities and the analysis of data-based representations of social reality in order to purposefully intervene into that reality (see, e.g., Pentland, 2015; Shah et al., 2015; Zysman and Breznitz, 2012).

These increased capacities together establish conditions under which it is possible to provide highly personalized and targeted solutions or treatments (products, services, etc.) to individual wants and desires on a massive scale (Newell and Marabelli, 2015). An illustrative example of this capacity of individualized treatment is based on large amounts of highly detailed health data in the area of medicine. With ever more detailed information about individual patients, more personalized treatments can be administered. While the new information infrastructure, hence, allows for managing greater complexity, the decentralized coordination on which it is based involves a radical individualization and stronger role of individuals as coproducers of the products, services, and solutions

they receive (Sharon, 2017: 95). They are asked to provide inputs (information, demands, etc.) and to react to inquiries and decisions that form part of a dynamic coordinative effort. Such an arrangement thus gives greater weight to individual activation and engagement. In doing so, it supports an extension of the principle of conditionality in the area of welfare.

A first way in which this extension of conditionality can take place is the more targeted intervention and structuring of incentives based on a more detailed picture of social reality. This basically amounts to enhancing previously existing administrative capacities through establishing informationally more demanding kinds of conditionality.More detailed information about individuals' conduct can serve to regulate their behavior by making benefits in one area dependent on their conduct in another area. Such a form of conditionality is visible with regard to Australia's lump-sum Maternity Allowance, which was originally provided to parents with the birth of a child and has become conditional on the full immunization of the child. As Henman (2011: 3) writes:

> over the last decade there has been a proliferation of public policies that cross over and connect two previously distinct policy domains. These policies are characterized by making eligibility for a service or benefit in one domain conditional on a circumstance or behavior in a second domain.

This is an illustrative but still relatively crude example of extended conditionality. The new ICT infrastructure allows for much more targeted structuring of incentives based on the notion that people, through adequate intervention, have to be moved to adopt habits and decisions that are deemed better and more rational (John, 2016; Oliver, 2015), e.g. with regard to education- (Bradbury et al., 2013) and health-related (Haydock, 2014) behaviors. A decade ago, Hood and Margetts (2007: 182) wrote that information technology would primarily enhance nodality/information as a tool and resource in the hands of governments, and particularly its use as a detector. However, as governments' new technological tools allow for a more targeted introduction of behavioral incentives, these resources can increasingly operate as effectors. The social credit system introduced in China that makes various options and benefits for citizens conditional on a comprehensive history of their previous behaviors and their compliance with legal rules as well as professional and social standards (Chen and Cheung, 2017) is arguably the most radical and most striking example in that regard.

Such intricate and indirect ways in which conditionality can be extended in the welfare state are based on increased capacities for monitoring individual behavior. There is a rapidly growing literature concerned with self-tracking that points to how digital technologies can bolster conditionality (Crawford et al., 2015; Fotopoulou and O'Riordan, 2017; Lupton, 2016; Sanders, 2017; Sharon, 2017). On the one hand, the growing abilities to track and assess the minutiae of individual behavior produce new forms of knowledge about the self that can help people to gain more awareness over their habits and lifestyle, which may ultimately enhance control over their life. On the other hand, digital self-surveillance can have disempowering effects through disciplining individuals to self-regulate their behavior in accordance with existing power structures. In combination with prevalent ideals of being a productive and valuable member of society, the constant awareness of how an individual and its own conduct compares to extant norms and expectations encourages ongoing self-discipline, self-regulation, and self-optimization in order to meet those ideals (Fotopoulou and O'Riordan, 2017: 58–59; Lupton, 2014: 79; Sanders, 2017: 10–11). As Sharon (2017) shows in her study, it is ultimately an empirical question which form this takes in actual practice, and such normalizing effects may not actually occur given that digital technologies can be appropriated in various ways. However, a general tendency in these self-tracking practices is that they strengthen the role of personal responsibility and encourage individuals to take care of themselves.

This stronger emphasis on individual responsibility forms an important basis for strengthening conditionality, individualizing protection from risks, and legitimizing cutbacks in the welfare state based on the ideas of empowered and self-reliant patients who are enabled to care for themselves (Fotopoulou and O'Riordan, 2017: 63; Sharon, 2017: 101–102). Moreover, insurances have begun to make more individualized offers, promising lower rates and premiums that are conditional on health-related behaviors registered through individual self-tracking; and companies have an incentive to introduce conditionality of rewards and provisions through exacting individuals to track their productivity- and health-related behaviors (Lupton, 2014, 2016; Moore and Robinson, 2015; Morozov, 2014: 237; Whitson, 2013).

The increased capacity of tracking individual behavior and quantifying personalized risks as well as individual efforts to manage these risks not only matters for disciplining and regulating behavior through conditionality but it also has important consequences for conceptions of reciprocity and solidarity. The social institution of insurance is inherently related to technology as it is based on the technical abilities to estimate risks (Lehtonen and Liukko, 2011; McFall, 2015)—and with the availability of fine-grained representations of

social reality, these abilities are considerably enhanced. The more it becomes possible to perform highly individualized risk assessment and corresponding pricing, the more this goes against certain conceptions of how risks should be shared (McFall, 2015: 41). More personalized risk assessments are more in line with chance solidarity (Lehtonen and Liukko, 2011: 38), which implies that risks and contributions are made commensurate and contributions are tied to risk categorizations. More personalized risk calculations reduce uncertainty and make possible discriminations that were not detectable previously. They thus establish distinctions where individuals could be counted as equals before, and even though risk pooling may still take place, such practices are harder to reconcile with those forms of solidarity (Lehtonen and Liukko, 2011: 39; Rosanvallon, 2013: 211–213) that disregard personal distinctions when answering the question of how risks and contributions are to be shared. Instead, they place a greater emphasis on individual responsibility and meritocratic thinking as a basis of conditionality in the protection from risks. Overall, the discussed cases show that digital technologies generally sustain a greater emphasis on individual activation and responsibility in managing existential or welfare risks and allow for creating new forms of conditionality that shift risks to the individual. The changing information infrastructure, however, is not only relevant for the question of conditionality in the context of the welfare state but the principle of conditionality also extends to the area of privacy and data protection, as the next section argues.

Conditionality in data collection and processing

The political economy of data-centered value creation

Issues associated with digital technologies, their adoption and use have so far hardly become politicized. Yet, there is very much something at stake for policy actors due to the way these technologies sustain profound changes in industrialized economies. Not only is there a growing importance of the ICT sector in general, but also data and specifically data about individuals' (and their devices') activities have turned into a valuable raw material (Srnicek, 2017: 25–26). Networking, mobile, and sensor technology have made it possible to cheaply and unobtrusively collect such data in a highly distributed fashion. In combination with techniques for generating insights from data, those possibilities furthermore contribute to personal data being regarded as resource comparable to oil in the early 20th century (Helbing, 2015: 75). This changed status of data has led to attempts to assess the economic value of personal data[1] (OECD, 2013), and there is a rapidly increasing number of contributions that deal with how businesses can create value from data and establish data-driven business models (e.g., Akter and Wamba, 2016; Brownlow et al., 2015). Businesses, including beyond the ICT sector, are compelled to draw on data as a raw material in various ways, be it for optimizing business planning and processes, analytical purposes (e.g., real-time monitoring), developing new products and services, as well as for a more efficient and highly personalized marketing (Akter and Wamba, 2016; Brownlow et al., 2015; Curry, 2016; Lambin, 2014).

Hence, an economic sector is taking shape, in which value creation is based on collecting and processing data about individuals' behaviors and dispositions as a raw material. A report by the European Parliamentary Research Service (Davies, 2016) states that businesses in the field of data analytics alone could add 1.9% to GDP between 2014 and 2020 in the European Union. Governments of various industrialized countries now openly acknowledge the relevance of this economic activity. The British government, for instance, has called it one of its most important sectors (DCMS, 2017), and a strategic note by the European Commission (2017) on the ''Data Economy'' sees data as ''bedrock of the future economy'' that determines the success of business and future prosperity of economies. In sum, data-driven economic value creation is rapidly gaining importance for countries' economic development, especially as the digital sector is growing faster than the average economy in times of overall low growth (Colecchia et al., 2014: 13, 37). As the data economy depends on the availability and access to personal data, governments need to provide a suitable environment in which data-driven business can flourish (see, e.g., Davies, 2016: 7) if they want to harness the economic potential of these activities. Governments face strong incentives to do so because they can be expected to be judged by voters according to the economic performance they are associated with (Easton, 1975; Scharpf, 1999). Hence, if they do not want to put economic growth and international competitiveness at risk they are likely to support an environment favorable to data-driven business.

The impetus to foster the widespread collection and processing of data about individuals' behaviors and dispositions faces obstacles, however. Value creation based on data as a raw material involves making use of its unprecedented granularity by generating insights that were formerly not possible. Highly detailed representations of behaviors, habits, and decisions serve to quantify individuals' existences with regard to many aspects. For companies, the categorization and further analysis of these representations for the purposes of sorting and prediction are a major means for obtaining

a competitive edge (Akter and Wamba, 2016; Cavanillas, 2015). On the one hand, this allows businesses to offer highly personalized solutions and to better accommodate and even anticipate customer desires which are, in fact, an outspoken goal of major internet companies (see, e.g., Wakabayashi and Barr, 2015). On the other hand, these capabilities entail an asymmetric increase of information power of some organizations, and the orientation toward data as core resource and raw material to be employed in value creation is prone to turning consumers into a resource or commodity (Crain, 2016; Lyon, 2003; Martin, 2015: 76; Scherf, 2008: 50). Not only are they harvested as objects of data collection, but the aim of inference and preemption based on unobtrusive data collection may also negate the agency and subjectivity of these data objects (Hildebrandt, 2011; Rouvroy, 2013). This can take the form of a paternalistic relation in which individuals may be rewarded and reinforced if they behave according to the predictions and suggestions tailored toward them (Andrejevic, 2007).

The social importance of data-driven business models, hence, extends beyond merely the economic realm as it touches upon and may get into conflict with a moral and political ideal of personal autonomy which is hard to reconcile with possibly paternalist and objectifying practices of data collection and processing. It is thus important to look at how autonomy, personal responsibility, and conditionality are constituted in an emerging data economy.

Conditionality and personal responsibility in the data economy

Looking at the status of individuals as data subjects in current approaches toward privacy and data protection, one can detect a great weight being placed on individual agency and personal responsibility in managing risks of data exposure. Particularly in the United States, self-management and informed user consent have been guiding principles in people's interactions with data collecting organizations (Solove, 2013). Informed consent puts the burden on the individual to control which personal data he or she discloses and under which conditions. As a number of authors have forcefully argued, this principle is oblivious to the ways in which the standard of informed consent is extremely demanding (e.g., Cohen, 2012; Scherf, 2008; Solove, 2013). Behavioral economics has shown that in their managing of personal data individuals often fall prey to cognitive biases that lead them to act against their actual preferences and best interest (Brandimarte and Acquisti, 2012; Solove, 2013: 1888–1889). Moreover, while individuals generally value privacy and data protection highly, they do not generally act in line with these attitudes (Compañó and Lusoli, 2010; Hallinan et al., 2012; Lusoli et al., 2012; Norberg et al., 2007). The bottom line is that reliance on individual responsibility can hardly assure that individuals are autonomous subjects in how they deal with and control their personal data. Nonetheless, privacy and data protection are to a large degree a matter of self-management, and it is still valid to say that "[p]rivacy self-management takes refuge in consent" (Solove, 2013: 1880). The strong emphasis on self-reliance with regard to privacy and data protection still holds in the USA, even after the 2015 US Consumer Privacy Bill of Rights Act (Baruh and Popescu, 2017: 585).

The ideas of individual responsibility and self-reliance, however, are not specific to the US. They even inform the European Union's comparatively restrictive General Data Protection Regulation, which enters into force in May 2018. This legislation contains some far-reaching novelties, such as restrictions for corporate actors through the required transferability of data and the provision of tools for local (instead of cloud) storage of data. At the same time, it emphasizes giving the individual more capacities to exert control over his or her personal data, e.g. through greater transparency and more effective possibilities for opt-outs. On the one hand, this means people are given better means for exercising control over their own data-based representations. On the other hand, the General Data Protection Regulation also shifts responsibility to citizens and emphasizes individual control, mainly to be realized through suitable technical tools (Costa, 2017; Crabtree et al., 2016: 950–951; Koops, 2013: 200). Rubinstein (2013: 2–3) argues that EU data protection still heavily relies on the idea of informed choice. He goes on to emphasize that the core principles of European data protection law are likely to remain ineffective because they require that people are aware of their data being processed and (are motivated to) make use of their rights while the massive proliferation of data, its analysis and new applications heighten the challenge of making informed choices (Rubinstein, 2013: 5–7). Moreover, as long as citizens are provided with the means to obtain information that, however, do not shed light on how personal data about them are used to produce certain decisions, the transparency offered through data protection provisions is only of a nominal character (Ananny and Crawford, 2016; Koops, 2013: 205).

Hence, as Crabtree et al. (2016: 947) note, privacy and data protection regulation "shifts the locus of agency and control in data processing towards the individual consumer." Such an arrangement, however, risks to perpetuate citizens' vulnerabilities.[2] More responsibility for the individual may seem desirable, but in order for them to become autonomous data

subjects, they also need to be empowered through means that allow for effectively exercising such autonomy. This would require a corresponding institutional setting in which the data subjects become real stakeholders (De Vries, 2013: 25), are capable to exert control over their data, and assume a position in which they can bargain with data collectors on a level playing field.[3] This would stand in stark contrast to the practice that has been prevailing to date, in which ''participating'' in and reaping the benefits of the data economy is based mainly on consenting to give away data in exchange for ''free of charge'' services and content.

All in all, extending the means and increasing the capacity for achieving transparency and control over one's personal data does not mean that individuals' autonomy is actually strengthened. Rather, responsibility lies with the individuals to take action. In that sense, the current approach to privacy and data protection introduces as specific form of conditionality: If citizens do not take action to exert control over their data, the fault for unwanted outcomes ultimately lies with them, as they essentially had the means necessary to prevent data collection and uses against their interest. This may include serious cases of harm through cyber crime, but it also more generally comprises practices of data collection and processing that users would find unacceptable or undesirable.

This form of conditionality resembles the one described above in the context of the welfare state; it establishes a relation in which a person is seen as deserving of protection if he or she shows a certain conduct, i.e. makes use of available means to realize control over his or her data. Understood as a policy tool, this conditionality equally establishes the protection from certain risks as a question of individual responsibility and tends to discard structural barriers to realizing the ideal of self-reliance. Like in the area of welfare, it encourages, but also requires individuals to make use of opportunities for protecting themselves from disadvantages. At the same time, the latent assumption that control over one's data essentially is as a matter of personal will and effort discards the importance of structural conditions that would allow individuals to achieve such autonomy. Failing to achieve the desired control can then only have been the result of insufficient effort.

However, the motivation and probability of success for individuals' efforts to manage their data-related risks are slim in light of structural barriers that are easily dismissed by foregrounding individual responsibility and self-reliance. The data economy is hardly geared toward individuals and is essentially dominated by businesses (Cohen, 2012; Rubinstein, 2013). Data, technology, and specialized knowledge are accumulated by economic entities, which altogether leads to increased asymmetries toward consumers and citizens. Growing amounts of data and increasing sophistication in extracting insights from this data further contribute to these asymmetries. Moreover, it seems doubtful whether the intricacies of algorithmic data processing can be made intelligible to citizens/consumers even where trade secrets would allow that. The complexity of the dynamically adapting algorithmic processing and categorization based on multiple data sources means that individuals cannot effectively challenge these processes. Baruh and Popescu (2017: 591) thus conclude in their study that ''the algorithmic social sorting characteristic of big data environments drastically limits the ability of individuals to self-define, and thus claim control and agency, over their social trajectory.'' Following Tene and Polonetsky (2013: 255), these circumstances can be likened to a poker game in which one player can see the other players' cards.

In order to better grasp how this impinges on individual agency, the concept of autonomy specifically understood as nondomination, as the absence of arbitrary rule (Pettit, 1999), is particularly instructive. According to Pettit (1999), freedom as noninterference is limited by any kind of interference, even one that is in accordance with one's interests (e.g., accepted rules or laws). At the same time, such a nonarbitrary limitation, e.g. through laws, does not have to constitute a form of domination. In contrast, individuals exposed to the power of others to arbitrarily interfere with one's choices do not entertain freedom as nondomination. A slave, for instance, can have a benign master and be free from interference but will still be subject to domination because someone else is ultimately in control. Similarly, where information power is used to preempt individuals' decisions and to structure the options and conditions under which they decide, freedom as nondomination is violated. The individual may even perceive an absence of interference and experience satisfaction based on his or her decisions but he or she is nevertheless subject to domination exerted through information power.

Altogether, to the extent that information power based on personal data is used to circumvent any dialogical relation with others (Hildebrandt, 2011) individuals are treated as mere objects and denied a status of moral subjects. Respecting this status presupposes acknowledging a person's ability to make reasoned and deliberate, and in that sense autonomous, choices. Clearly, people's reasoning is never free in the sense that it occurs in a vacuum and unaffected by any external influences. However, the kind of information power described above is a power to arbitrarily interfere directly into that reasoning, and individuals may thus not be able to tell whether and how (the presentation of) their options and choices have been purposefully

structured by others. The ability to change a range of options and the ways they are presented "affect the domain of options available to you or affect our capacity to deliberate within that domain" (Pettit, 2015: 383). This is different from persuasion, which still has a dialogical character and acknowledges a deliberative capacity.

These considerations have important implications for how governments are likely to shape not only their policies but also their justifications in governing the data economy. On the one hand, there are strong incentives to create a favorable environment for the data economy. On the other hand, as this activity touches on major normative ideas, policy actors face legitimatory pressures that they will have to address if they want to promote such an environment.

Legitimizing a data-driven economy

The previous section has pointed to a legitimatory challenge which policy actors face because of a tension that exists between two ends: They have to reconcile economic incentives to foster data-centered value creation, on the one hand, with normative ideas deeply ingrained in liberal democratic regimes, on the other hand. Policy actors have been shown to fall back on established ideas and frames of references in dealing with such legitimatory pressures (Abdelal et al., 2010; Blyth, 2003; Hall, 1993). A suitable template stems from the area of welfare reforms, where governments have been able to put more weight on market principles and introduce conditionality while accommodating an ideal of agency that emphasizes individual responsibility. Similarly, as governments aim to create the conditions under which a data-driven economy can flourish, the more they are likely to emphasize that protection from risks related to data exposure are not unconditional and that privacy and data protection are a matter of individual responsibility. This would allow for removing obstacles standing in the way of data flows and data processing for economic value creation while still adhering to the idea of autonomy.

In order to probe how governments legitimize developing the data economy, the following account looks at developments in the United Kingdom and Germany by drawing on relevant policy documents and government communication. There are several reasons why these two countries are particularly relevant cases. Not only have both countries updated their initial digital strategies from 2013 with a number of programs and initiatives by 2017 but they are also in many ways different cases. This is important because if similar tendencies in the legitimizing rhetoric around decisions regarding the digital sector and data-driven business are observable in both countries, this only underscores a more general impetus to push the boundaries of a data economy. Germany is a continental country with a strongly consensual political system and a coordinated market economy (Hall and Soskice, 2001), and it is furthermore known for a comparatively restrictive approach to privacy and data regulation, in large part due to judgments by the German Federal Constitutional Court (Cremer, 2011). The United Kingdom, in contrast, belongs to the Anglo-Saxon family of nations (Castles and Mitchell, 1993), has a liberal welfare state and market economy, following a stronger pro-market approach. Moreover, it has been quick to invest into the ICT infrastructure (Hanna, 2016), particularly in the financial sector (Harcourt, 2016), and also been a very early adopter of far-reaching video surveillance in the public. The ICT sector is furthermore likely to gain considerable importance in the UK. Especially after the Brexit, the country is forced to adjust and reorient its economic model and strategy, and the ICT sector plays an important role in that overall readjustment. The Cameron government and the May government have expressly stalled the publication of an already overdue strategy for the digital economy in face of the Brexit uncertainties (Broersma, 2017). The greater importance of this economic activity in the UK and the generally greater emphasis on market forces suggest that the British government is more likely to take a light-touch approach with regard to data collection and processing and give a more prominent role to personal responsibility.

Turning first to the UK, the update of the digital strategy has to be seen against the backdrop of years of a rapidly growing tech and ICT sector. Since the digital strategy of 2013, several reports by the government and parliament were published that documented a stunning growth and future prospects of that sector (see, e.g., Select Committee on Digital Skills, 2015); the Cameron government came to recognize a need to tap data as a major resource for economic value creation. As the government (DBIS, 2015) stated in its UK vision for a digital economy:

> Of course new technologies bring new risks, so we need to set data protection in a broader framework that ensures the security of citizens. But the proliferation of data is inevitable. If we don't create the right climate for seizing the opportunities this brings, we can be confident that data-driven innovation will continue elsewhere and simply be sold into the EU.

The updated digital strategy put forward by the May government has addressed that challenge. The strategy contains one section specifically about the "data economy," which is entitled "Unlocking the power of data in the UK economy and improving public confidence in

its use'' (DCMS, 2017). This part of the digital strategy acknowledges the importance of transforming the UK into a ''world-leading data-driven economy'' in order to achieve sustainable growth.

The strategy, thus, sees the use of data as a raw material essentially as a way to tap a further source of wealth, and the government aims to create suitable conditions for realizing this economic potential. For this purpose, corresponding possibilities for harnessing data flows, making possible innovative uses, and performing data analytics have to be opened up. In this context, it is notable that the UK Digital Strategy 2017, unlike the previous digital strategy (Cabinet Office, 2013), expressly characterizes data as a ''global commodity''—a depiction that suggests few needed restriction for dealing with this resource. Moreover, the increased impetus to push the boundaries of a data-driven economy has been supplemented with a reframing of the envisioned role that individuals as data subjects take in this value creation. The digital strategy contains a part that is entitled: ''Supporting people's data rights and responsibilities.'' This heading is particularly noteworthy because—again unlike in the previous digital strategy—the government is expressly taking up the notion of responsibilities. The digital strategy stresses that the government ''also need[s] people to play their part in keeping their information secure'' and that individuals have to be encouraged to ''take responsibility for their own data, particularly in the online environment'' (DCMS, 2017). The government has thus given a prominent place to individual responsibility concerning individuals' status as data subjects. Through asking individuals to play an active role in controlling the way in which their data is collected and processed, there is a visible parallel to a welfare state discourse that emphasizes personal responsibility with an important difference being that the idea of conditionality is not openly expressed with regard to control over one's data. The conditionality in the area of data collection and processing is, however, still left implicit and amounts to a protection from informational risks that are premised upon showing a—hardly defined—capacity and competence in dealing with one's own data.

A similar trend is observable in Germany, where the government too has acknowledged the importance of data-driven business models. The recent White Book on Digital Platforms, for instance, states that an ''innovative, data-centered economy with a strong industrial basis forms the European model for securing wealth'' (BMWI, 2017, own translation). There are thus clear incentives for policy actors to create a favorable environment for such a data-centered economy.[4] Indeed, the government has on various occasions admonished that too strict data protection and privacy laws may threaten the development of new business models, innovation, and the country's competitiveness. The former Minister of the Economy Sigmar Gabriel thus pleaded for replacing the notion of data protection with that of data sovereignty (''*Datensouveränität*'') on the IT summits of 2015 and 2016 (Die Zeit, 2016; Gabriel, 2015)—a concept and guiding idea that has since been recurring in policy documents concerned with the digital economy. Gabriel also stated (as did the Minister for Traffic and Infrastructure Alexander Dobrindt) that data minimization could not continue to be a guiding principle and that it would threaten the country's international competitiveness. Instead of aiming for minimization and data parsimony (''*Datensparsamkeit*''), a mentality of ''data wealth'' was to be established, thus directly linking the proliferation of data with desirable economic outcomes.

In November 2016, Chancellor Angela Merkel reiterated that in light of an inevitable massive proliferation of data and data exposure, data sovereignty was a more suitable concept than data protection. She emphasized that the principle of data minimization did not suit new forms of value creation, and that the European privacy and data protection rules should not be translated into national law in a way that would be too restrictive for data-driven business (Deutschlandfunk, 2016). In early 2017, the government presented a revised draft for adapting the national data protection law. The draft contained softened reporting obligations of data collectors and aimed to weaken the requisite that data cannot be appropriated for other purposes than for which it was originally collected. The government's plans were met with resistance by a number of organizations, experts, and the data protection commissioner, which eventually led to changes in the adopted law. Nevertheless, there has been a shift in the policy trajectory, especially given that data minimization and tying data use to a predetermined purpose have so far been key principles of the German data protection approach. Also, the notion of data sovereignty has been established as a major guiding idea. This idea has taken on an ambivalent character in the way it has been used by the German government. While this conception of sovereignty openly aims to promote the autonomy and protection of consumers and citizens, it also locates responsibility to a greater extent in the individual. What this data sovereignty implies can be read from policy documents that are concerned with fostering a data-driven economy. It basically amounts to enabling individuals to develop relevant competences needed for having control over one's data. As the German Digital Strategy 2025 (BMWI, 2016) posits, digital core competencies and abilities are to be identified and promoted in order to systematically generate and maintain digital

sovereignty. Citizens are thus not per se given protection and guarantees of their informational autonomy. Rather, they are to be enabled to actively take care of their data exposure.[5] This emphasis on citizen activation essentially shifts risks that may occur as a consequence of data collection and processing to the individual citizen.

Altogether, in both examined countries one can witness a change in the guiding ideas that govern the policy-making and rhetoric regarding data flows, collection, and processing—a change that is most noticeable in Germany, where the government has openly discarded the notion of data protection and instead pleaded for data sovereignty. Both cases are marked by attempts to promote a greater role for a data-centered value creation that are furnished with a greater emphasis on individual responsibility as a legitimizing idea. The examined government action thus resembles the way that conditionality is used as a policy tool and legitimatory device in the politics of the welfare state. The principle of conditionality takes precedence over guarantees, and essentially the same ''artificially individualized and rationalized'' (Wright, 2012: 322) conception of agency and motivation that is present in welfare policy focused on work first and strong conditionality is taking hold in the governing of the data economy.

Accordingly, safeguarding privacy and data protection is modeled after a contract with rights and responsibilities which implies that citizens are not per se the recipients of certain protections and guarantees by the state but are only deserving of protection if they take responsibility themselves. It is then also fitting that a greater focus in the examined digital strategies lies on developing the competences deemed necessary to act as an autonomous subject in the data economy. Like in the area of welfare (see, e.g., Wright, 2012), however, such a focus on personal qualities and capacities stems from a reductionist vision of individual agency that presumes a self-reliant individual detached from its social and institutional context. At the same time, this conception of individual agency and emphasis on individual responsibility work as a normative justification. Stressing the importance of individual conduct allows to partly absolve the state from responsibility—if individuals do not make use of available options to secure their privacy and personal data, it can be attributed to their lack of initiative. This way, a normative idea of autonomy can be reconciled with leaving more scope for practices of value creation based on personal data as a raw material.

The reasons why conditionality and the idea of individual responsibility appear to take a similar place in the data economy as in certain welfare state policies can be seen in a common impetus to extend market forces into social relations. As conditionality commodifies individuals in the welfare state, it also commodifies personal data as well as the carriers of that data in their role as data subjects through exposing them to market relations. Despite the similarity in how conditionality operates in the two areas, there is, however, also an important difference. Activation in the welfare state and encouraging people to become productive members of society is generally desirable from the point of view of the national economy. In contrast, the economic potential of the data economy is more easily realized the less individuals care to take control over their data so that data as a raw material can more easily be tapped.

Conclusion

Advances in ICTs and their widespread adoption lead to a profound transformation in societies' information infrastructure that is marked by a networked and highly decentralized monitoring and coordination of activities—of humans and machines alike. The result is a leap in the capacities for managing complexity that makes possible significant efficiency and productivity gains. This information infrastructure and ambitions to make use of these capacities, it has been argued above, sustain functionally related developments in two different policy areas regarding the regulation of individual behavior. First, the changed information infrastructure supports an already existing tendency in the area of welfare to establish conditionality, which ties benefits to certain forms of individual conduct. The extension of conditionality regarding protection from welfare risks is made possible through the individualizing potential of ICTs, based on a much more fine-grained tracking of behavior that is carried out by the individuals themselves. This enables more and more specific required forms of conduct, to make use of new possibilities for self-management, and to build on more personalized risk assessments—all forms of conditionality that emphasize individual responsibility and operate through disciplining standards and ideals that govern personal conduct.

Conversely and second, establishing conditionality in the area of data protection serves to unlock the capacities of the changed information infrastructure for economic purposes. Conditionality in this respect involves the notion that it is an individual's own responsibility to show a certain conduct and to make use of formal opportunities for safeguarding one's privacy and personal data. Data protection thus becomes individualized and data subjects are placed within market relations in the context of an emerging ''Data Economy'' (European Commission, 2017). This is important because less rigid guarantees and protections free up data flows that provide the raw material for the

value creation in that economy. This conditionality and the concomitant emphasis on individual responsibility are not only present in existing data protection laws, but it also guides how the development of the data economy is governed and justified. The developments in the UK and Germany examined above show how governments stress conditionality in the area of data protection. Governments in both countries have, in their updated digital agendas from 2017, shifted responsibility for the protection of personal data away from the state and established data protection as a question of not only rights but also individual responsibilities. This marks a change in emphasis and in the approach toward data protection as policy actors depict informational autonomy less as something that is to be guaranteed but that instead should be conditional on certain forms of individual agency. Similar to how conditionality operates in the context of welfare, conditionality in the area of data protection has been legitimized by invoking the normative idea of personal responsibility and an ideal of human agency that stresses self-reliance but tends to blend out the role of structural preconditions for realizing autonomy.

This way of reconciling normative ideas with extending practices of value creation based on personal data addresses an important challenge that policy actors face. Governments of industrialized countries openly acknowledge the importance of exploiting data as a raw material for economic growth and future international competitiveness. However, as they advance their digital strategies and aim to harness the economic potential of data, they run into legitimatory pressures because the collection and processing of personal data can have commodifying effects and subject individuals to power asymmetries that impinge on their personal autonomy. In view of such pressures, policy actors are likely to fall back on already existing and familiar legitimizing ideas that have been used for comparable challenges. The principle of conditionality in the welfare state provides a suitable template in that context as it allows for championing a conception of human agency that can help to legitimize policy change which puts a greater weight on personal responsibility.

Unlike welfare issues, however, value creation centered on processes of data collection and processing has so far hardly been politicized. There are some reasons why this could change in the near future. After all, the regulation of value creation based on data as a raw material has immediate consequences for people's protection from risks and inconveniences that result from practices of data collection and processing. Moreover, policy actors are compelled to push harder for opening up data flows and ways of data processing if they want to reap the economic potential of the data economy. Politicized or not, as technological conditions change and as the growing importance of data-centered value creation pushes policy actors to create a favorable environment for this economic activity, they can hardly avoid to renegotiate the role of individuals in the data economy and the risks to which they are exposed.

Acknowledgments

I would like to thank the reviewers for their helpful comments and suggestions. Thanks also go to Rebekka Kugler, who has helped with the preparation of the manuscript.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. Personal data is usually understood as data that can be attributed to an individual and comprises, e.g. preferences, dispositions, and behaviors. However, the requirement of identifiability is becoming meaningless to the extent that the identity of a person can be determined with very high accuracy from assembled pieces of information that are individually not identifying (Rubinstein, 2013). It can furthermore be useful to broaden the concept of personal data to individuals' personal devices since these operate as their agents and thus enact their preferences and intentions.
2. Moreover, this data protection approach leaves room for—and may even reproduce—inequalities with regard to data subjects' vulnerabilities (see also Madden et al., 2017). Their technological sophistication matters for the degree to which they are capable of managing their data exposure. Moreover, if data and its collection and use are monetarized, privacy and data protection can become a question of whether a person is able to afford it. While some people will be ready to spend extra money for their privacy and a better protection of their data, others simply put up with being harvested for data if they want to partake in the data economy. In a similar vein, the protection of one's data is also likely to depend on its economic value, with e.g. financial and health data—which are of course also more sensitive—being very valuable, receiving better protections and being more likely to be remunerated. Finally, whereas citizens have to actively exert control if they want to protect their data, corporate actors enjoy guaranteed protections. For instance, algorithms, which ultimately are data too, are granted special protection already for proprietary reasons; most government data, despite widespread Open Data initiatives, remain well entrenched.
3. Some authors envision these relations through the creation of intermediating tools that empower data subjects as vendors of their data so that data collectors have to request

and bid for that data (e.g., Crabtree et al., 2016; Rubinstein, 2013: 9–13).

4. It should be noted that political actors too—where it is legal—have a vested interest in availing themselves of massive amounts of fine-grained voter data in the context of election campaigns and political marketing: for more potent techniques of voter analysis and micro-targeting (Bimber, 2014).
5. These kinds of risks predominantly relate to the more palpable criminal uses and abuse of personal data. There is, in contrast, little about more subtle ways in which data may be used against individuals treating them in ways that deny their agency.

References

Abdelal R, Blyth M and Parsons C (eds) (2010) *Constructing the International Economy*. Ithaca, NY: Cornell University Press.

Akter S and Wamba SF (2016) Big data analytics in E-commerce: A systematic review and agenda for future research. *Electronic Markets* 26(2): 173–194.

Ananny M and Crawford K (2016) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*. Epub ahead of print: 13 December 2016. DOI: 10.1177/1461444816676645. Available at: http://journals.sagepub.com/doi/abs/10.1177/1461444816676645.

Andrejevic M (2007) Surveillance in the digital enclosure. *The Communication Review* 10(4): 295–317.

Baruh L and Popescu M (2017) Big data analytics and the limits of privacy self-management. *New Media & Society* 19(4): 579–596.

Bennett WL and Segerberg A (2012) The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication & Society* 15(5): 739–768.

Bimber B (2014) Digital media in the Obama Campaigns of 2008 and 2012: Adaptation to the personalized political communication environment. *Journal of Information Technology & Politics* 11(2): 130–150.

Blyth M (2003) Structures do not come with an instruction sheet: Interests, ideas, and progress in political science. *Perspectives on Politics* 1(4): 695–706.

BMWI (2016) *Digitale Strategie 2025*. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BMWI (2017) *Weißbuch Digitale Plattformen. Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe*. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

Bonoli G and Natali D (eds) (2012) *The Politics of the New Welfare State*. 1st ed. Oxford: Oxford University Press.

Bradbury A, McGimpsey I and Santori D (2013) Revising rationality: The use of ''nudge'' approaches in neoliberal education policy. *Journal of Education Policy* 28(2): 247–267.

Braman S (2006) *Change of State: Information, Policy, and Power*. Cambridge: MIT Press.

Brandimarte L and Acquisti A (2012) The economics of privacy. In: Peitz M and Waldfogel J (eds) *The Oxford Handbook of the Digital Economy*. New York: Oxford University Press, pp. 547–571.

Broersma M (2017) Government blames Brexit for digital strategy delay. *Silicon*. Available at: http://www.silicon.co.uk/e-regulation/government-blames-brexit-digital-strategy-203508 (accessed 3 November 2017).

Brownlow J, Zakl M, Neely A, et al. (2015) *Data and Analytics – Data-Driven Business Models: A Blueprint for Innovation*. Cambridge: Cambridge Service Alliance.

Cabinet Office (2013) *Government Digital Strategy: December 2013*. London: Cabinet Office. Available at: https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy (accessed 3 November 2017).

Castles FG and Mitchell D (1993) Worlds of welfare and families of nations. In: Castles FG (ed.) *Families of Nations: Patterns of Public Policy in Western Democracies*. Aldershot: Dartmouth Publishing Company, pp. 93–128.

Cavanillas J (2015) *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*. New York: Springer Berlin Heidelberg.

Chandler D (2015) A world without causation: Big data and the coming of age of posthumanism. *Millennium* 43(3): 833–851.

Chen Y and Cheung ASY (2017) *The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System*. Hong Kong: University of Hong Kong. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992537 (accessed 3 November 2017).

Cohen JE (2012) *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press.

Colecchia A, et al. (2014) *Measuring the Digital Economy: A New Perspective*. Paris: OECD.

Compañó R and Lusoli W (2010) The policy maker's anguish: Regulating personal data behavior between paradoxes and dilemmas. In: Moore T, Pym D and Ioannidis C (eds) *Economics of Information Security and Privacy*. Boston, MA: Springer US, pp. 169–185.

Costa L (2017) *Virtuality and Capabilities in a World of Ambient Intelligence: New Challenges to Privacy and Data Protection*. New York: Springer.

Cox RH (2001) The social construction of an imperative: Why welfare reform happened in Denmark and the Netherlands but not in Germany. *World Politics* 53(3): 463–498.

Crabtree A, et al. (2016) Enabling the new economic actor: Data protection, the digital economy, and the Databox. *Personal and Ubiquitous Computing* 20(6): 947–957.

Crain M (2016) The limits of transparency: Data brokers and commodification. *New Media & Society* Epub ahead of print 7 July 2016. DOI: 10.1177/1461444816657096. Available at: http://journals.sagepub.com/doi/abs/10.1177/1461444816657096.

Crawford K, Lingel J and Karppi T (2015) Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies* 18(4–5): 479–496.

Cremer H-J (2011) *Human Rights and the Protection of Privacy in Tort Law: A Comparison Between English and German Law*. London; New York: Routledge-Cavendish.

Cukier K and Mayer-Schoenberger V (2013) The rise of big data. How it's changing the way we think about the world. *Foreign Affairs* 28(3): 28–40.

Curry E (2016) The big data value chain: Definitions, concepts, and theoretical approaches. In: Cavanillas J, Curry E and Wahlster W (eds) *New Horizons for a Data-Driven Economy*. Cham: Springer International Publishing, pp. 29–37.

Davies R (2016) *Big Data and Data Analytics. The Potential for Innovation and Growth*. Brussels: European Union.

DBIS (2015) *UK Vision for the EU's Digital Economy*. London: Department for Business and Innovation & Skills and Prime Minister's Office. Available at: https://www.gov.uk/government/publications/the-uks-vision-for-the-european-unions-digital-economy/uk-vision-for-the-eus-digital-economy (accessed 3 November 2017).

DCMS (2017) *UK Digital Strategy 2017*. London: Department for Culture, Media & Sport. Available at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy (accessed 3 November 2017).

Deutschlandfunk (2016) Merkel regt Lockerung der Datenschutzregeln an. *Deutschlandfunk*. Available at: http://www.deutschlandfunk.de/it-gipfel-merkel-regt-lockerung-der-datenschutzregeln-an.1818.de.html?dram:article_id=371663 (accessed 3 November 2017).

De Vries K (2013) Privacy, due process and the computational turn: A parable and a first analysis. In: Hildebrandt M and de Vries K (eds) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Milton Park: Routledge, pp. 9–38.

Die Zeit (2016) Gabriel mahnt zu mehr Daten-Souveränität. *Die Zeit*. Available at: http://www.zeit.de/news/2016-11/17/internet-nationaler-it-gipfel-beraet-ueber-digitale-bildung-17054005 (accessed 3 November 2017).

Easton D (1975) A re-assessment of the concept of political support. *British Journal of Political Science* 5(4): 435–457.

European Commission. (2017) Enter the data economy. EU policies for a thriving data ecosystem. *EPSC Strategic Notes* 21: 1–16.

Fotopoulou A and O'Riordan K (2017) Training to self-care: Fitness tracking, biopedagogy and the healthy consumer. *Health Sociology Review* 26(1): 54–68.

Gabriel S (2015) Gabriel mahnt zu mehr Daten-Souveränität. *Deutschlandfunk*. Available at: http://www.deutschlandfunk.de/sigmar-gabriel-wir-brauchen-die-vorratsdatenspeicherung.868.de.html?dram:article_id=314247 (accessed 3 November 2017).

Hall PA (1993) Policy paradigms, social learning, and the state: The case of economic policymaking in Britain. *Comparative Politics* 25(3): 275–296.

Hall PA and Soskice DW (eds) (2001) *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press.

Hallinan D, Friedewald M and McCarthy P (2012) Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review* 28(3): 263–272.

Halvorsen K (1998) Symbolic purposes and factual consequences of the concepts ''self-reliance'' and ''dependency'' in contemporary discourses on welfare. *Scandinavian Journal of Social Welfare* 7(1): 56–64.

Hanna NK (2016) *Mastering Digital Transformation: Towards a Smarter Society, Economy, City and Nation*. Bingley: Emerald Group Publication.

Harcourt A (2016) Communications policy in the European Union: The UK as a policy entrepreneur. In: Zahariadis N (ed.) Handbook of Public Policy Agenda Setting (Handbooks of Research on Public Policy). Cheltenham; Northampton: Edward Elgar Publishing, pp. 332–347.

Haydock W (2014) The rise and fall of the ''nudge'' of minimum unit pricing: The continuity of neoliberalism in alcohol policy in England. *Critical Social Policy* 34(2): 260–279.

Helbing D (2015) *Thinking Ahead – Essays on Big Data, Digital Revolution, and Participatory Market Society*. Cham: Springer International Publishing.

Hemerijck A (2013) *Changing Welfare States*. Oxford: Oxford University Press.

Henman P (2011) Conditional citizenship? Electronic networks and the new conditionality in public policy. *Policy & Internet* 3(3): 71–88.

Hilbert M and Lopez P (2011) The world's technological capacity to store, communicate, and compute information. *Science* 332(6025): 60–65.

Hildebrandt M (2011) Who needs stories if you can get the data? ISPs in the Era of big number crunching. *Philosophy & Technology* 24(4): 371–390.

Hood C and Margetts H (2007) *The Tools of Government in the Digital Age*. Basingstoke: Palgrave Macmillan.

John P (2016) Behavioral approaches: How nudges lead to more intelligent policy design. In: Peters BG and Zittoun P (eds) Contemporary Approaches to Public Policy: Theories, Controversies and Perspectives (International Series on Public Policy). London: Palgrave Macmillan, pp. 113–131.

Kitchin R (2014) Big data, new epistemologies and paradigm shifts. *Big Data & Society* 1(1). Available at: http://bds.sagepub.com/lookup/doi/10.1177/2053951714528481 (accessed 25 May 2016).

Koops B-J (2013) On decision transparency, or how to enhance data protection after the computational turn. In: Hildebrandt M and de Vries K (eds) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Milton Park: Routledge, pp. 196–220.

Kurzer P (2013) The politics of ideas in reforming the Dutch disability fund: Reforming the disability fund. *Governance* 26(2): 283–305.

Lambin J-J (2014) A digital and networking economy. In: *Rethinking the Market Economy*. London: Palgrave Macmillan UK, pp.147–163.

Lehtonen T-K and Liukko J (2011) The forms and limits of insurance solidarity. *Journal of Business Ethics* 103(S1): 33–44.

Lupton D (2014) *Self-Tracking Cultures: Towards a Sociology of Personal Informatics*. OzCHI '14 Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: the Future of Design: 77–86. Available at: https://dl.acm.org/citation.cfm?id=2686623 (accessed 3 November 2017).

Lupton D (2016) The diverse domains of quantified selves: Self-tracking modes and dataveillance. *Economy and Society* 45(1): 101–122.

Lusoli W, et al. (2012) *Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management*. Brussels: European Commission.

Lyon D (2003) Surveillance as social sorting. Computer codes and mobile bodies. In: Lyon D (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London; New York: Routledge, pp. 13–30.

McFall L (2015) Is digital disruption the end of health insurance? Some thoughts on the devising of risk. *Economic Sociology the European Electronic Newsletter* 17(1): 32–44.

Madden M, Gilman M, Levy KEC, et al. (2017) Privacy, poverty and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review* 95: 53–129.

Martin KE (2015) Ethical issues in the big data industry. *MIS Quarterly Executive* 14(2): 67–85.

Moore P and Robinson A (2015) The quantified self: What counts in the neoliberal workplace. *New Media & Society* 18(11): 2774–2792.

Morozov E (2014) *To Save Everything, Click Here: Technology, Solutionism and the Urge to Fix Problems That Don't Exist*. London: Penguin Books.

Newell S and Marabelli M (2015) Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of ''datification''. *The Journal of Strategic Information Systems* 24(1): 3–14.

Norberg PA, Horne DR and Horne DA (2007) The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41(1): 100–126.

OECD (2013) *Exploring the Economics of Personal Data*. Paris: OECD. Available at: http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (accessed 27 July 2015).

Oliver A (2015) Nudging, shoving, and budging: Behavioral economic-informed policy. *Public Administration* 93(3): 700–714.

Pentland A (2015) *Social Physics: How Social Networks Can Make Us Smarter*. New York: Penguin Books.

Pettit P (1999) *Republicanism: A Theory of Freedom and Government*. Oxford: Oxford University Press.

Pettit P (2015) Freedom: Psychological, ethical, and political. *Critical Review of International Social and Political Philosophy* 18(4): 375–389.

Rosanvallon P (2013) *The Society of Equals*. Cambridge, MA: Harvard University Press.

Rouvroy A (2013) The end(s) of critique: Data behaviorism versus due process. In: Hildebrandt M and de Vries K (eds) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Milton Park: Routledge, pp. 143–167.

Rubinstein IS (2013) Big data: The end of privacy or a new beginning? *International Data Privacy Law* 3(2): 74–87.

Sanders R (2017) Self-tracking in the digital era: Biopower, patriarchy, and the new biometric body projects. *Body & Society* 23(1): 36–63.

Scharpf FW (1999) *Governing in Europe: Effective and Democratic?*. Oxford: Oxford University Press.

Scherf R (2008) Yes I agree*: Assessing the failure of ''privacy self-management'' and its regulatory reforms. *Public Policy and Governance Review* 6(2): 37–54.

Schram SF and Soss J (2001) Success stories: Welfare reform, policy discourse, and the politics of research. *The ANNALS of the American Academy of Political and Social Science* 577(1): 49–65.

Select Committee on Digital Skills (2015) *Make or Break: The UK's Digital Future*. London: House of Lords. Available at: https://www.publications.parliament.uk/pa/ld201415/ldselect/lddigital/111/111.pdf (accessed 3 November 2017).

Shah DV, Cappella JN and Neuman WR (2015) Big data, digital media, and computational social science: Possibilities and perils. *The ANNALS of the American Academy of Political and Social Science* 659(1): 6–13.

Sharon T (2017) Self-tracking for health and the quantified self: Re-articulating autonomy, solidarity, and authenticity in an age of personalized healthcare. *Philosophy & Technology* 30(1): 93–121.

Solove D (2013) Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review* 126(7): 1880–1903.

Soss J, Fording RC and Schram S (eds) (2011) *Disciplining the Poor: Neoliberal Paternalism and the Persistent Power of Race*. Chicago, IL; London: University of Chicago Press.

Srnicek N (2017) *Platform Capitalism*. Cambridge: Polity.

Svensson J (2011) Power and participation in digital late modernity: Towards a network logic. In: Tambouris E, Macintosh A and de Bruijn H (eds) *Electronic Participation*. Vol. 6847. Berlin, Heidelberg: Springer Berlin Heidelberg, pp.109–120.

Tene O and Polonetsky J (2013) Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property* 11(5): 240–273.

Wakabayashi D and Barr A (2015) Apple and Google know what you want before you do. *The Wall Street Journal*. Available at: http://www.wsj.com/articles/apple-and-google-know-what-you-want-before-you-do-1438625660 (accessed 3 November 2017).

Whitson JR (2013) Gaming the quantified self. *Surveillance & Society* 11(1/2): 163–176.

Wiggan J (2012) Telling stories of 21st century welfare: The UK Coalition government and the neo-liberal discourse of worklessness and dependency. *Critical Social Policy* 32(3): 383–405.

Wright S (2012) Welfare-to-work, agency and personal responsibility. *Journal of Social Policy* 41(2): 309–328.

Zysman J and Breznitz D (2012) Double bind: Governing the economy in an ICT era. *Governance* 25(1): 129–150.